REMARKS

This paper is in response to the Office Action of June 28, 2005. The due date for response extends to September 28, 2005.

The Applicants appreciate the Examiner's indication that the Objections under 35 U.S.C. § 132 have been withdrawn.

Examiner's Interview Summary

The Examiner is thanked for extending the undersigned the courtesy of a telephone interview on August 26, 2005. In the interview, the a discussion was had regarding the teachings presented by Bruce Schneier, Applied Cryptography, 1996, pages 31-32, 39, 176-177, and 357-360 (hereinafter referred to as "Schneier"). A discussion was also had with regard to Uranaka et al. (US Pat. 6,470,085).

Firstly, the undersigned pointed out that Schneier is broadly concerned with the basics of communication using Public-Key Cryptography (PKC). The Applicants invention is not attempting to claim PKC *per se*, but alternatively, the use of PKC in accordance with a methodology, as defined in the independent claims. To this end, the defined use of the PKC, as is commonly taught and implemented is to create a key pair defined by a public key and a private key. The public key is made available to some third party, and that that third party can use the public key to encrypt some data that is intended for the holder of the private key. Following this functionality, Schneier notes that is best to place the public key on some database, and that public key could be made available to members of the public for subsequent encryption of data to a given holder of the private key (i.e., the holder of the complementary asymmetric key). Schneier further goes on to define other encryption processes, including double and triple encryption, which can use one or more encryption algorithms.

An important aspect to take from Schneier's teachings, is that the encryption is performed using one or more public keys, and each public key is created without regard to the user that will ultimately use the public key. Contrary to this teachings and basic common understanding of PKC, the claimed invention generates the public key/private key pair for a particular user. See Fig. 2B. This detail was discussed with the Examiner in the telephone

conference. To more fully define this distinction, the Applicants suggested a clarifying amendment to the independent claims. As provided in this amendment, the clarification makes clear that the public key is generated or created for a given user, in response the initiated access request.

The Examiner further referred to Uranaka et al., which has been discussed and addressed in past Office Actions. The Examiner's office action relies on Uranaka et al. in combination with Schneier, under a 35 USC § 103(a) rejection. For the additional reasons, some of which were discussed with the Examiner, the rejection is respectfully traversed.

The Examiner also noted that Uranaka et al. is different from the claims invention in that Uranaka et al's double encryption is not asymmetric. This clarification was also added to claims 88 and 100. The other independent claims are clear on their own, that the double encryption is asymmetric.

Also, Uranaka et al. does not generate a user public key for a user, as defined in the pending claims.

Reference should be made to column 2, lines 33-36, where it is stated that "...the key is first obtained in a user public key-encrypted from the DVD on which the key has been recorded at the time of selling the DVD." This teaching is on its face contrary to the claimed invention. If the user public key is recorded on the DVD at the time of selling the DVD, then the user public key cannot be generated or created *using* the user information.

Reference should also be made to column 8, lines 38-41, where it is noted that "...the server public key (PKs) contained in the distribution descriptor 23 recorded in the burst cutting area of the DVD with the ID and the network address." It is made certain here, that the "server public key is contained ON the DVD before it is sold. It therefore follows that the each of the user public key and server public key is created in advance of knowing who the ultimate user might be.

A question thus remains regarding the complementary "private keys." The private keys, referred to as "secrete keys" by Uranaka et al., are in fact not involved in the creation nor generation for a particular user. The opposite is in fact true. The Examiner is kindly referred to column 18, lines 42-46, where Uranaka et al. states that "one who is permitted to use an application package is limited to an owner of the IC card which stores a user secrete

key Sku corresponding to the user public key PkU used for encryption of the AP-encrypting key Kv in the application package."

Taking the teachings of Uranaka et al. as a whole, Uranaka et al. teaches a system where a packaged media (with pre-generated public keys) is sold with an IC card (with pre-generated private keys). The holder of the IC card has the key to open the DVD, and if some unauthorized users comes in contact with the DVD, they will not be able to decrypt the contents, as they may not possible have the IC card.

Combining the teachings of Uranaka et al. with Schneier fails to teach or suggest each and every element of the claimed invention. This is especially true taken that Uranaka et al. fails to teach the user specific generation of user public key/private key pairs, and Schneier teaches pre-generated of non-user specific public keys stored on databases.

For at least the foregoing reasons and those noted in the telephone interview, the Examiner is respectfully requested to withdraw the rejections to the pending independent claims. The dependent claims are submitted to be patentable for at least the same reasons the independent claims are submitted to be patentable.

A Notice of Allowance is therefore respectfully requested.

If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 749-6903. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SONYP007). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

Albert S. Penilla, Esq.
Reg. No. 39,487

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Facsimile: (408) 749-6901
Customer No. 25920